InfoTrust

THE ULTIMATE GUIDE TO COMPLIANT TRACKING: GOOGLE ANALYTICS 4

Lucas Long
Tag Governance Specialist

InfoTrust

THE ULTIMATE GUIDE TO COMPLIANT TRACKING: GOOGLE ANALYTICS

Lucas Long is a Senior Tag Governance Specialist and Product Manager at InfoTrust, working with global organizations at the intersection of privacy regulations and technical tag management. Through these efforts he helps global organizations across verticals ensure complete and compliant data collection.

Lucas Long
Tag Governance Specialist
taginspector.com/contact/

Table of Contents

I. Privacy Implications of GA4 (pg. 3-4)

II.User Consent and Opt-Out (pg. 5-13)

- ePrivacy Directive (EU "Cookie Laws")
- GDPR
- CCPA
  - Block GA from executing and collecting any information for users that opt out
  - Stop GA from collecting "personal information" for users that opt-out
  - Stop GA from the "sale" of personal information for users that opt-out
- Mechanisms Available
  - Disable Analytics Data Collection
  - Disable Google Signals Data Collection
  - Disable Advertising Personalization

- **Transparency and Disclosure (pg. 13-14)**
- **User Access & Deletion Requests (pg. 15-17)**

- Data Access
- Data Deletion

V. Privacy by Design quests (pg. 18-19)

- IP Anonymization
- Data Retention
- Remember, No PII in Google Analytics!
- Data Sharing Settings
- Data Processing Amendment

InfoTrust

THE ULTIMATE GUIDE TO COMPLIANT TRACKING: GOOGLE ANALYTICS

I. Privacy Implications of Google Analytics

Tag Inspector is a tag auditing and monitoring platform designed for marketing, analytics, and governance pros. If you manage a large site or multi-brand enterprise, Tag Inspector's comprehensive tag library and suite of auditing functionality provides unparalleled confidence that your data is complete, compliant, and efficient across your organization.

taginspector.com

Last quarter, we published the first "Ultimate Guide to Compliant Tracking for Google Universal Analytics." Shortly after (on Oct. 14, to be exact), Google announced the next version of Google Analytics, Google Analytics 4. As many organizations will be migrating to the new version throughout 2021, we felt it important to update and expand on the compliant tracking guide specifically for Google Analytics 4.

Let's take a deeper dive, shall we?

As we have previously outlined, we like to think about privacy requirements through a simplified lens. To do this, consider these four "sections":

1. **Privacy by design**
2. **Transparency and disclosure**
3. **User consent and opt-out**
4. **User access and deletion**

To start, let's explore how a standard "out of the box" implementation of Google Analytics 4 (known colloquially as GA4) works, and then the privacy implications that result. From there we will surface all relevant information for each of our four sections of privacy requirements.

[For some background context, it might be helpful to review what tags are, what cookies are, and how it all works.]

With GA4 specifically, when a user comes to your website, the following happens:

1. A user comes to a webpage with a GA4 tag implemented.
2. When the webpage loads in the user's browser, the browser will execute (or "fire") the GA4 tag.
3. When the GA tag is fired, it will do a few things (generally):
   1.) Set on the user's browser a few standard, first-party cookies for user behavior tracking functionality after reading the tag, and
   2.) compile and send a network request to Google Analytics servers containing data used for analytics.

From a privacy and compliance perspective, there are some implications due to this behavior.

First, due to the placement and accessing of cookies on the user's browser, the base configuration will fall in the scope of cookie laws in a number of countries. Most notably, this puts GA4 in the scope of the ePrivacy Directive (and country-specific laws flowing from it) within Europe.

The ePrivacy Directive has requirements along the main categories of our simplified privacy framework mentioned earlier: privacy by design, transparency and disclosure, user access and deletion, and user consent and opt-out.

In addition to the privacy implications related to the storage and accessing of information from a user's device (which GA4 will be doing in the form of cookies each time the GA4 tag loads), there are also requirements related to the collection of data. The requirements for data collection are outlined in legislation such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act).

[*For a deep dive into the requirements around marketing and advertising data collection for GDPR check out this guide; for CCPA this webinar will be helpful*]

Regardless of any custom configuration you are doing that may result in additional privacy considerations, default out-of-the-box GA4 data collection includes some parameters that will be relevant. The most applicable of which is the Device ID.

The Device ID is a unique, anonymous identifier that is created and persists for each and every device that visits your website. Now, before you finish yelling that "devices are not users", consistent guidance and judgments from data protection authorities across the globe have refuted that argument, so it is best we move from rage to acceptance.

Google Analytics 4 will both store this value in one of the cookies they set, as well as collect this data point in every hit sent. The ID is used to anonymously identify a user in order to stitch together hits and user actions across a site, app, and devices. Device ID is also important to be able to associate campaign information that brings a user to the website with resulting events and conversions. Without this ID, all you will have are general counts for events—no user nor attribution reporting would be possible within analytics.

This natively-collected data point can be interpreted as falling within the definition of "personal information" for CCPA and, depending upon what you are doing with the GA4 data down-stream internally, the definition of "personal data" as defined in GDPR. Custom parameters configured to be collected may also be collecting data falling within these definitions. Consult with your in-house legal teams to make this distinction for your organization.

As a result of these data points (and their privacy implications due to meeting the definitions of personal information/personal), you will need to make sure you are following the requirements for disclosure, access, and user choice as outlined in any applicable privacy laws.

Let's now dive into Google Analytics. We'll use our simplified privacy framework to organize the exploration.

II. User Consent & Opt-Out

This is the area that brings the most questions. (And with consent requirements varying from regulation to regulation and country to country, it's no wonder.) Let's first discuss the user consent requirements for each of the main privacy regulations most organizations will be considering: ePrivacy, GDPR, and CCPA.

ePrivacy Directive (EU "Cookie Laws")

The restrictions with respect to consent and user choice vary a bit from country to country. Some countries will require explicit affirmative consent prior to the placement or accessing of any cookies on the user's browser, while others have some carve-outs in this requirement for analytics platforms (such as just basic GA4 tracking). Here you'll want to consult your organization's legal council to determine how they want to interpret each country's laws. It is important to note that exceptions for consent with respect to analytics platforms only apply if you are not using any additional advertising features associated with GA4 (we'll get to this shortly).

As a general rule, most countries in Europe have legislation that requires explicit consent prior to the placement or accessing of cookies for analytics purposes. For Google Analytics 4, since those default cookies are going to be placed whenever the GA4 tags execute, this means that the Google Analytics 4 tags should not fire until a user has explicitly consented to tracking. The implication of this for your analytics reporting is that no data will be collected for those users that do not consent, nor will data be collected for consenting users until they give an affirmative consent indication. Compared to historical numbers in your reporting, there will be a drop in the amount of data being collected; we usually see a 40-60% reduction in the volume of visitors tracked once explicit consent is implemented.

As mentioned, there are some countries with exceptions to this requirement. Consult with your legal team to determine your final approach.

General Data Protection Regulation (GDPR)

GDPR defines "personal data" as any data point that can be used to directly or indirectly to identify a natural person. With Google Analytics 4, the Device ID that is collected in all hits sent to GA may be considered "personal data," depending upon what you are doing with the data.

As previously discussed, the Device ID is a unique, anonymous ID that persists and is associated with a user's device. On its own, it cannot be used to identify a natural person, but if it is being used as part of a larger data set that contains more user information from other sources, it potentially can be. The most-likely risk here is if you have Google Analytics 4 linked to other advertising platforms and are using audiences from GA4 for targeting.

Generally, if you do not have Google Signals data collection enabled within GA4, are not linking your Google Analytics 4 properties with Google Ads, and are only using the data in analytics for aggregate statistical reporting purposes, then it's possible that no GA4 data will be classified as "personal data" and therefore the principles of GDPR will not apply. This also assumes you are not collecting any "personal data" in custom parameters associated with events, either.

However, if you are leveraging any of those other features or are using GA4 data to supplement advertising datasets, it is likely that the Device ID *will* fall under this "personal data" definition. Not to mention, if you are collecting a User ID in Google Analytics 4, then that could likely fall under this definition as well.

Ultimately, the core GDPR principle to understand is that all personal data must have a legal basis for processing. This can be obtained through either consent or legitimate interest. In most cases, organizations are relying on consent for the use of Google Analytics 4 data in this way.

When relying on consent as the legal basis for processing, in order for that consent to be valid under GDPR, users need to provide explicit affirmative consent prior to any processing of their personal data. Therefore, no "personal data" can be collected by Google Analytics 4 until explicit consent has been granted by the user. To satisfy this, organizations have a couple technical mechanisms they can leverage.

1. **Disable Google Analytics from firing for users until they consent.** Here you would not be collecting any data, and therefore run no risk of processing "personal data". The implication for analytics reporting again is that nothing will be collected unless a user consents to tracking, resulting in less data than in the past when all users were tracked.
2. **Allow Google Analytics to fire and collect aggregate statistical data, but do not collect "personal data" until the user consents.** As mentioned above, the data collected in GA for standard reporting does not contain the context necessary to directly nor indirectly identify a natural person. The risk is introduced with potential custom dimensions/metrics you may be collecting and when GA is linked with other platforms where that data is then combined with other datasets. It is therefore possible to conditionally omit the collection of any custom metrics/dimensions until a user consents to this processing as well as to conditionally disable advertising features in Google Analytics. The technical mechanisms for doing this are outlined later in this document.

California Consumer Privacy Act (CCPA)

The CCPA provides additional rights for California-based users with respect to their "personal information." Personal information is defined in the CCPA as any data point that can be associated with an individual or household. For Google Analytics 4, the client ID that is being sent in every hit is a unique identifier associated with a user. Due to this, GA4 is always going to fall within the scope of CCPA.

For user choice, CCPA carries the requirement to provide users the ability to opt-out of the sale of any personal information. As established, Google Analytics 4 will be collecting and processing "personal information," but depending upon what you are doing with that data, you may not be "selling" the information as that action is defined in the law. Generally, if you are only using GA data for reporting purposes within Google Analytics, then you wouldn't be "selling" any of this data. If you have GA linked with other Google Ads products and are creating audiences to share across platforms, then you may fall under the "sale" definition. (Again, you should work with your legal counsel to determine if this is the case and if the opt-out requirement applies.)

If the opt-out requirement does apply, then you have a few of options for how to comply with it:

1. Block Google Analytics from executing and collecting any information for users that opt-out.

This is the most common approach, the most conservative from a compliance perspective, and the most straightforward from a technical standpoint. To do this, you will use one of the three options for disabling analytics data collection that we will outline below.

2. Stop Google Analytics from collecting "personal information" for users that opt-out.

For this, you will need to do a CCPA evaluation for Google Analytics and first identify all the data points that would fall under the "personal information" definition. At minimum, you will be dealing with the Device ID.

As of today, there is not a simple out-of-the-box method to disable the collection of the Device ID. There is a beta feature called "Consent Mode" that restricts GA4's use of cookies and some data collection when an indication of consent has not been given. We will provide additional updates as we learn more information about this feature.

To address any other datapoint that you may be collecting due to additional custom configuration, you would need to implement a mechanism to not collect those parameters for users that have opted out. An example of a common data point where this would apply that many organizations collect is User ID.

3. Stop Google Analytics from the "sale" of personal information for users that opt-out

CCPA defines the sale of personal information as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

Many legal groups are interpreting this definition to cover the transfer of personal information from analytics to advertising platforms. As a result, if a user opts out, you would likely need to stop these transfers from happening. Again, if you do not transfer Google Analytics data to any other locations, do not have GA linked with Google Ads, and are not creating and transferring audiences in GA to advertising platforms, then this "sale" definition would likely not apply. Where it does, Google has now introduced some technical mechanisms to remove individual users' data from being transferred out of Google Analytics. We cover these mechanisms (disabling advertising features and disabling ad personalization) later in this document.

By implementing these measures, you could likely have a defensible position for compliance with the opt-out requirements. I want to again emphasize that you **need to discuss these approaches with your own legal counsel** to align with their interpretations and levels of risk acceptance. The only sure-fire approach is to stop the execution of Google Analytics for users that have opted-out of the sale of their personal information. If none is collected, it cannot be sold.

Now that we understand the opt-out requirements as outlined in the main privacy regulations we need to comply with, you may be thinking that analytics is a thing of the past in this new privacy environment. Fear not! There are a number of approaches that you can take to still collect the data you need to drive your business while still respecting the privacy of your users.

Mechanisms Available

Let's explore some of the technical options Google Analytics provides to limit data collection. What exactly can we disable (what choice can we give to users) and what does disabling each mean?

Disable Analytics Data Collection

Disabling analytics data collection generally can be accomplished in a few different ways. The first, and most likely to be used, is to not execute the Google Analytics tag implemented on the website. The technical mechanism to not execute (or block) the GA4 tag will vary depending upon your specific architecture. The most likely solutions are:

1. **A Consent Management Platform (CMP) implementation.** In this scenario, you would have a consent management system implemented on your website to manage the consent experience of users. Based upon the consent selection by the user, the CMP will make an indication (or consent selection flag) available. This will either be via a cookie that the platform places on the user's browser or via an indication in a JavaScript object (or data layer) on the page. Regardless of the consent indication method, you would need to configure the firing rules ("triggers" if using Google Tag Manager) for the Google Analytics 4 tag to have a condition looking for the consent indication to be true. If that indication is not present, the GA4 tag would not execute and no data would be collected nor cookies set.
2. **A custom-built consent solution.** This scenario would follow the same logic as the first. The only difference would be that instead of a consent management platform providing the indication of consent, some other custom logic or code on your site would be doing so. You still would add logic to the execution rules for the Google Analytics 4 tag to not fire unless the consent indication is affirmative. The same scenario of GA4 only firing after consent has been given results.
3. **A window property added to the Google Analytics script to indicate that measurement should be disabled.** This approach is outlined in the Google Universal Analytics support documentation. Basically you are adding a line to the GA4 tag script [before any calls to the 'gtag()' function are made] to indicate that the GA4 property should be disabled. When this condition is set to 'true', the GA4 tag will not execute. The 'true'/'false' indication needs to be made conditional based upon the consent indication of the user.

In any of the above situations, Google Analytics 4 is not going to run the function to send data. The result is that no data will be collected, no cookies will be set by GA4, and the user would not be tracked at all. For complete opt-out, this would be the solution. This also needs to be the default behavior (GA not running at all) for users in locations where explicit consent is required for data collection or for the placement and/or accessing of cookies. Once explicit affirmative consent has been granted, then GA can be executed.

[Bonus note: Users also have the ability to opt-out of all GA tracking for any/all websites via the Google Analytics opt-out browser add-on. If a user has this installed, it will disable execution of any Google Analytics JavaScript tags (gtag.js, ga.js, analytics.js, and dc.js).]

Impact on Analytics

When any of these methods are used, the Google Analytics 4 tag will not execute when user consent has not been granted (or a user has opted-out). Because the GA4 tags do not fire, those users will not be tracked at all in your GA reporting, nor will any cookies be set on the users' browsers. Again, we usually see a 40%-60% reduction in data when this type of explicit consent mechanism is introduced.

Disable Google Signals Data Collection

You may be used to the terminology of "Advertising Features" from Google Universal Analytics. "Google Signals" was introduced in 2018 as the method to use within GA for cross-device reporting. This feature allows for aggregate data from users that have allowed "Ads Personalization" within their own Google Ads account settings to enhance the data you have collected directly. From Google, "Google signals is a cross-platform measurement feature with optional advertising applications." Here's the full breakdown for what is possible within GA4 with respect to Signals.

Before we discuss disabling Signals in Google Analytics 4, it's important to understand a little more context about what we are disabling. An explicit explanation for how Signals functions is not yet published for GA4, but borrowing from the description for Universal Analytics, "analytics can collect information about your users from the Google advertising cookies when they are present, along with the information Analytics normally collects."

Put simply, when you disable Signals in Google Analytics 4, the GA4 tag will not read from and collect additional information from other Google advertising cookies present on the user's browser, and users will not be able to be used in audience lists shared with other linked advertising platforms (including remarketing audiences).

Google Signals can be enabled (and disabled) from within the UI in the GA4 Property Settings or via a script modification in the GA4 tag being used to collect data. Given these multiple approaches, you have the ability to disable Signals both for an entire property or for individual users.

To disable Signals for an entire property, you will go into the 'Admin' section of your GA4 Property and toggle off the "enable Google signals data collection" in your data settings. More than likely, an organization will want to have these on (so you take advantage of all GA functionality for consenting users). Still, it's important that organizations can dynamically disable the data collection for individual users that are opting out.

To disable Google Signals data collection for individual users, you will need to do the following:

1. Make sure that Google Signals for data collection is enabled at the Property level in the Admin settings. are enabled at the Property level in the Admin settings.
2. Update your Google Analytics 4 tracking code to include an additional field to set setting 'allow_google_signals' to 'false' for users that have not granted consent and/or opted out. Conversely, you would need to set this field to 'true' for users that have granted consent. Here's Google's documentation for how to do so for a GA4 tag. Also helpful is this documentation, which outlines the approach to take across various implementation types (including GA4 template tags used in GTM).

[A really important note: The true/false value that needs to populate the 'allowAdFeatures' field will be dynamic based upon the consent indication of the user. How you will determine this is going to depend upon the consent mechanism that you have in place. Ultimately you will be looking for the same consent indications as outlined in the methods to disable analytics data collection. In this scenario, however, you will be using those indications to dynamically update the value of this value as opposed to dynamically executing or not executing the Google Analytics tag. If you need help with this logic and implementation, contact our team.]

Impact on Analytics

Dynamically disabling Google Signals data collection for specific users will have a few impacts:

1. Users with this indication will not be included in remarketing audiences that are shared with other linked Google Ads platforms.
2. Users with this indication will not be able to be used to create segments based upon their demographic and interest data (i.e., they are not included in segments to use to create look-alike audiences).
3. GA4 will not collect additional information about these users from other Google advertising cookies on their browser. Therefore, demographic and interest data will not be available for these users (i.e., they will not show up in Audience Demographics and Interests Reporting). They will not show up in Display & Video 360 reporting available in GA4 and they will not show up in Google Display Network Impression Reporting in GA4.

In summary, for users with this option dynamically disabled, standard aggregate reporting in Google Analytics will still include the actions of these users (events, eCommerce, etc.) but none of the advertising features will include these users in reporting nor actions.

[Important Note from Google regarding the enabling of Signals data collection: "Enabling reports is contingent on reaching a monthly average of 500 users per day per property. Analytics will regularly check the size of clients and enable reporting support once a property has reached that daily average of users over the last 30 days. Reports remain enabled if you subsequently drop below that average." This is to ensure the supplemental information remains aggregate and statistical in nature to protect the privacy rights of individuals.]

Disable Advertising Personalization

Advertising Personalization is a feature component of Signals in Google Analytics 4. When Google Signals data collection is enabled on an account, Advertising Personalization is also enabled by default. This allows you to "collect data for ads personalization purposes, in addition to measurement, in connection with your use of such features as Google signals, User ID, ads integrations, and/or if you enable data sharing with Google" (from Google's documentation). In effect, it is the sub-section of the advertising features which contains all functionality related to leveraging data collected in Google Analytics 4 for personalized advertising to those users.

To translate this into practical terms, it is a sub-classification made in order to allow you to take advantage of reporting in Google Analytics 4 related to advertising integrations and supplemental Google Ads data. It allows you to exclude users from actions that could be interpreted as falling within the scope of "sale" as defined in CCPA. If you remember from the above discussion of the "sale" of "personal information" under CCPA, users have the right to opt out of these actions but that opt out right does not extend to collection nor processing. By including this disable ability specific to ads personalization, GA allows you to still collect data for all users, have reporting, and even supplement your collected data with aggregate ads data via Google Signals, while dynamically giving users the ability to opt-out of activities protected by CCPA.

Google Analytics gives you a couple of options for disabling Advertising Personalization:

1. Disabling for all users in a defined region.

To disable Ads Personalization for all users in a defined region, you will use advanced settings within your Google Analytics Property Settings. At the time of this writing Google has 306 "regions" covering most global countries and then state-specific options for the United States.

2. Disabling dynamically for specific users based upon a consent and/or opt-out indication.

Dynamically disabling Ads Personalization is very similar to dynamically doing so for Google Signals more broadly. To do this you will need to set an additional field, 'allow_ad_personalization_signals' to either 'true (for users where this should be enabled) or 'false' (for users where it should be disabled) in your Google Analytics tracking script. Here is Google's documentation for doing so across various different analytics implementation types.

3. Disabling specific events and/or user properties from use in ads personalization.

A new feature specific to GA4 allows you to indicate specific events and user properties that should be excluded for use in ads personalization. This configuration is done from within the GA4 reporting interface. When viewing either All Events or User Properties you simply indicate those that should be excluded as "NPA". Doing so will reserve the indicated data for analytics purposes only.

Some impacts when disabling specific events and user properties are important to call out. From Google's documentation:

- If you exclude an event or user property from ads personalization, then any audience that is based on that data is not eligible for export from Analytics to any of Google's advertising products (e.g., Google Ads, Display & Video 360, Search Ads 360). This also applies to any audience whose component audiences are based on that excluded data.
- Audiences that include such events and user properties are still available within Analytics for use in reports, Analysis, and audience building, and can be exported to non-advertising products like Optimize and BigQuery.
- The individual events and user properties excluded from ads personalization are available for export to advertising products, though they cannot be used by those products to personalize ads.

Important notes:

- *The same callout applies for the values to be populated in this field as for the Advertising Features above. The true/false distinction will need to be dynamic based upon the consent/opt-out indication of the user. Configuration of this will depend upon your consent experience and mechanism used.*
- *Disabling Advertising Features will also disable Ads Personalization, regardless of the dynamic indication in this field. This does not apply in reverse. Disabling Ads Personalization will only disable the feature set associated with this classification, it will not disable Advertising Features in total.*
- *To enable Ads Personalization, Advertising Features must also be enabled.*
- *The setting takes effect for data collection going forward and does not retroactively apply to data previously collected.]*

Impact on Analytics

When Ads Personalization is disabled, reporting within Google Analytics will not be impacted. However, some abilities you have to action the data in Google Analytics will be limited:

Users indicated as not eligible for use for ads personalization (either due to region disabling or dynamic user disabling) will not be added to any lists that may be exported to linked ads accounts.
When ads personalization is disabled for locations and users, all events collected and associated will be marked as not eligible for use.
Put simply: Users or events with this disable indication and/or users from disabled regions will be indicated in the GA backend. Any user with this indication cannot be included in audience lists when they are shared across linked Google Ads platforms for targeting. User actions, demographic information, and interest information associated with these users will also be excluded from consideration when creating look-alike audiences for use in linked Ads Platforms.

These users will still show up in reporting within Google Analytics, and they can still be included in audiences that can be exported to platforms (such as Google Optimize) for content personalization and A/B testing.

III. Transparency and Disclosure

The requirements for Transparency and Disclosure vary from legislation to legislation (For a quick guide to requirements for CCPA and GDPR, download our disclosure checklist). Generally, you will need to disclose to users the fact that you are collecting their data, placing/accessing information from their device, their rights under applicable privacy laws, and provide specifics as to the protected actions you are doing. These disclosures will need to take place both at the point of collection as well as in a more comprehensive format in an easily accessible privacy notice/policy.

Ultimately, your legal team will need to write and approve your disclosures to users on your websites. To help with this process, you can aggregate information about what data is collected by Google Analytics on your digital properties, how that data is used, any other platforms the data is transferred to, and information about any cookies that are placed on a user's browser by the tag.

You can compile this information in an easily consumable format by undergoing a thorough governance audit for privacy and compliance.

[Need help with this process? Contact our team.]

A few important resources specific to Google Analytics that can help:

1. General data collection

1. New to GA4 is the automatic collection (and the ability to enable "enhanced tracking") of certain events (user actions). Here you can find a full list of these automatically collected actions.
2. More relevant to your privacy disclosures are the automatically collected User Properties also introduced with GA4. Here is a list of these properties collected without any additional scripting or customization necessary. An important note from Google is that data thresholds are applied to protect the identification of individual users. From Google's documentation: "Thresholds are applied to prevent anyone viewing a report from inferring the demographics, interests, or location of individual users. When a report contains Age, Gender, Interests, or Location, a threshold may be applied and some data may be withheld from the report. For example, if there are fewer than N instances of
Gender=male in a report, then data for the male value may be withheld."
3. A lot of the data you are likely collecting in Google Analytics 4 is going to be custom configurations (Custom Events & User Properties). These are not standard across all organizations so you will want to make sure that any documentation as to your organization's data architecture is consulted.

2. Cookie Information

1. Documentation for how Google uses cookies from Google: This is a general reference from Google's Privacy Notices about how they use cookies across their various platforms (including Google Analytics 4).
2. Documentation about the types of Cookies used by Google: General documentation from Google's privacy notices about the types of cookies that are used and some information for why.
3. Google Analytics-specific documentation about the cookies set, durations, and how each is used: This is technical documentation, but it outlines the specific cookies that are used by Google Analytics. Also included is further context for how/why each cookie is used, the functionality cookies are leveraged for, and the default durations for each cookie. While the linked page is from the Universal Analytics documentation, GA4 leverages the gtag.js method for execution. Cookie behavior for this method is also included in the linked page.

3. General Helpful Documentation

1. General Google Support article that outlines the privacy safeguards that they have in place for Google Analytics. This article either contains or links to other relevant articles for pretty much all questions a legal/privacy team will have about Google Analytics. A great reference to have handy when doing an evaluation to determine what needs to be disclosed to users regardless of the regulations that are relevant.
2. Policy requirements for Google Analytics advertising features: Google outlines some specific privacy policies that must be adhered to when using Advertising Features in Google Analytics. This documentation provides both relevant information to include in your disclosures as well as policies that you are agreeing to when you enable these features.

IV. User Access and Deletion Requests

Codified in regulations such as CCPA and GDPR are rights afforded to users around the ability to request, and receive, all of their personal data/personal information. They also have the right to request that any personal information/personal data you have collected and stored from them be deleted. Google Analytics has introduced technical mechanisms to do so in their platform over the past year:

Data Access

Google Analytics allows for an organization to pull event information for any given user identifier via both the interface as well as via BigQuery.

1. Pulling event information via the UI

To pull event information for any given user identifier via the UI you can use the User Explorer report or the User Activity report within Google Analytics 4. These features allow you to analyze and export event level data for a single user identifier. Typically this user identifier is either the User ID (if you have implemented this in your GA4 Property) or the Device ID (default option if you have not implemented User ID as a user property and configured on your website).

The User Explorer functionality in GA4 is within the "Analysis" section of reporting. Once there you will create a segment or filter to include just the user identifier for the requesting user. Then you'll export the results to provide to the user and satisfy their access request.

2. Integrate GA4 Properties with BigQuery

New to GA4 is that all users (even on free, non-360 accounts) can integrate their GA4 Properties with BigQuery to create full exports of all event data associated with all of their users in a single queryable repository. If you have this set up, you can then easily and programmatically access the data in a more scalable way.

Data Deletion

There are two general approaches to data deletion in Google Analytics. You can either delete all data associated with a defined field/dimension or delete all information associated with a defined user. Let's look at both and also explore when you might use each.

1. Delete Parameters Associated with an Event

The Data Deletion Request method is used when you are collecting some kind of PII or personal information generally in a parameter across some or all events. A common reason for this is due to the identification of personally identifiable information collection. This is a violation of Google's Terms of Service and can lead to deletion of all data collected in a Property.

PII can make its way into GA4 data collection through a number of ways, many of them innocent mistakes. Examples would be if emails are being added as a URL parameter due to some website functionality, users inputting PII into search boxes and/or form fields on your website, even PII being included in js error messaging due to integration issues. In any case, it is still a violation to be collecting and storing this information in Google Analytics.

To provide more granularity in selecting the data to be deleted, GA4 provides five different deletion options to delete parameter data associated with events and/or users:

- Delete all parameters on all events
- Delete all registered parameters on selected events,
- Delete selected parameters on all events,
- Delete selected parameters on selected events,
- Delete selected user properties

To use this method, you will use Admin functionality in the GA4 UI to indicate your deletion request. You specify the deletion type, start and end dates for deletion, specific data fields you want to delete, and can optionally define a value pattern to delete.

When the request is submitted, the data meeting the conditions for deletion will be initially just hidden from reporting for the first 7 days. This week's waiting period gives you time to make sure the request is not inadvertent and gives time to cancel the request if necessary. Following the initial 7-day "preview period," the deletion process will begin on the backend, meaning the request will no longer be able to be canceled. Admins of the Property will be notified when the deletion process has completed.

[Editor's note: Worried about PII being sent to Google Analytics 4 or any other tag on your site? Check out the PII monitoring functionality within Tag Inspector's Privacy & Compliance suite of reporting.]

2. Delete Data Associated with a User (or a Specified User's Data)

Google Analytics 4 provides two types of User data deletion: deletion of User Properties and deletion of Users.

New to GA4 is the concept of User Properties. These are parameters that are scoped to (associated with) the user being tracked. Some standard User Properties are always collected within GA4 while additional custom properties can be configured. Using the data deletion request functionality outlined above, you have the ability to delete data within a defined User Property for all Users. This deletion type does not remove all information about that user nor the actions that user has taken across your digital properties. Aggregate statistical information will remain, but the data populating a defined User Property will be deleted.

The second method of deletion is deleting a User from GA4. This type of deletion will be used when a user executes their "right to be forgotten" under privacy legislation such as GDPR or CCPA.

Similar to the methods available for user access requests, you can satisfy user deletion requests via both the Google Analytics 4 interface or an API.

Deleting User Data via the UI

To delete user data via the UI, you will again use the User Explorer report within the Analysis section of GA4. You will first need to know the user identifier for the user in question (either the User ID or Client ID depending upon your implementation). Using this user identifier you can filter the User Explorer report to find that user record and all associated data. There is an option within the report to 'Delete User'. Using this will delete all of the event data associated with the user identifier from the Google Analytics servers.

Deleting User Data via the API

Google Analytics has a User Deletion API that allows a GA Property owner to programmatically request deletion of all data associated with a specified user identifier. Again, you will need a user identifier to specify the associated records to delete. With the API you can use either the Client ID, User ID, or the App Instance ID. Here is Google's documentation for executing these requests. Some important notes from Google's documentation regarding data deletion requests:

- For user data deletion requests: Once deletion is requested, data associated with the user identifier will be removed from the Individual User Report within 72 hours, and then deleted from Analytics servers during the next deletion process. Deletion processes are scheduled to occur approximately every two months.
- If data has been exported outside of Google Analytics 4 they recommend you delete it there prior to making the GA4 deletion request. The data deletion request will only delete data in GA4 and not in BigQuery or other potentially connected products. You will need to delete data in these downstream connected locations separately.
- For deletion requests of data associated with a user property or event parameter: Due to the way GA aggregates data, you may see data deleted up to 3 days before and/or after the beginning and end dates selected.
- There are some caveats to the data deletion requests:
    - GA4 supports the deletion of active registered parameters. If you do not see the parameter you want to delete, it's possible that it is not or has never been registered.
    - When deleting data associated with a specified user property, not all properties are available to be selected. These include the default user properties automatically collected. Click here for the full list.
- There are impacts on attribution analysis when deletion requests are executed. From the documentation: "When a deletion is completed, from that point forward all historical campaign information is no longer available for attribution–that information will have been deleted. Attribution credit going forward could go to other campaigns (if any are available from first-party ad clicks, or new campaign information collected after the deletion) or it will be considered 'Direct'."

V. Privacy by Design

Beyond the specific requirements for consent & user choice, transparency & disclosure, and user access and deletion; it is also important to implement Google Analytics 4 with user privacy as a core focus. GA provides a number of features that should be considered in order to meet all relevant regulatory requirements as well as user expectations.

IP Anonymization

In past versions of Google Analytics, IP Anonymization was opt-in and had to be configured in your tracking script. With GA4, IP Anonymization is the standard and is always enabled. This represents a good step in providing a more privacy-friendly solution.

Data Retention

One of the principles of GDPR is that personal data must only be processed for the duration of the activity for which it was collected. You cannot store data for the sake of storing it. As a result of this requirement (and as a general best practice), thought should go into how long data is stored in Google Analytics 4 based upon your industry and use cases.

In GA4, retention of user-level data, including conversions is fixed at up to 14 months. For all other event data, you may choose either 2 months or 14 months as the length of retention.

A few important notes about the data retention functionality:

- Standard aggregated Google Analytics 4 reporting is not affected by the automatic data deletion at these retention periods.
- The retention period applies to user and event data associated with cookies, user identifiers (Device ID and User ID), and advertising identifiers (ie. DoubleClick cookies, Android's Advertising ID, Apple's Identifier for Advertisers).
- In GA4 properties, increasing the retention period is applied to data that has already been collected.
- If you reduce the retention period, all data that is beyond the new period length will be deleted in the next monthly deletion process.
- Whenever you modify the retention period, GA will wait 24 hours before implementing the change.

One final option related to data retention to note is that you can select to "reset on new activity." When this is "ON" it will extend the retention period of the user identifier with each new event from that user. To illustrate this, say you have a 14-month retention period applied. Any data associated with a user will be stored until 14 months following that user's last tracked event interaction with the site on which that GA4 Property is implemented. This applies only to user data.

No PII in Google Analytics!

As detailed above in the data deletion section, it is a violation of Google's terms of service to collect PII data in Google Analytics 4. To help with this, Google has a few recommendations for how to avoid sending PII to GA. There are also a number of articles out there for how to find and replace PII prior to it being sent to GA. However you are going about it, you need to do everything possible to restrict PII from being sent to GA4. **It's possible that GA will delete all of your data in any property where PII is found to be stored.**

If you do identify PII collected in your property, refer to the data Deletion Section above for how to remove the data.

Data Sharing Settings

Within your Google Analytics Account, you have the ability to enable or disable data sharing with Google for a few different purposes. Options include for benchmarking purposes, technical support, account specialists, and sales experts. While enabling any of these data sharing settings is not a big privacy concern, it may be something your legal team will want to disclose within the privacy notice to users. Important to keep in mind is that these settings are at the Account level and will be applied to all Properties that live within that Account.

Data Processing Amendment

Your legal team may require that you enter into a data processing agreement with Google, depending upon the location of your business and users. There are a few different ways in entering a data processing agreement. Consult this section of the Google Analytics support documentation for more specifics on this topic.

User privacy has rightfully become a primary concern for all teams dealing with data. Google Analytics 4 introduces a new measurement approach that puts privacy in a more central role in analytics. The event-based collection method opens a number of avenues for opportunity to enhance data collection and analysis while also satisfying the privacy concerns of users and regulators. We hope this guide can be a good reference point for all of your privacy questions and configuration configurations with GA4. If you need guidance and support on your journey to complete, compliant, and efficient data collection, don't hesitate to reach out to the Tag Inspector team.